IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KYLIE S., ANTHONY P., ANNA S. and GENA W., on behalf of themselves and as parents and guardians of their minor children, K.S., J.P., K.P., D.C., M.C., J.C., Z.W. and C.W., and on behalf of all other similarly situated individuals, Plaintiffs, v. PEARSON plc,; NCS PEARSON, INC.; and PEARSON EDUCATION, INC., doing business as Pearson Clinical Assessment Defendants.	)	Case No. 1:19-cv-5936 Judge John Z. Lee Magistrate Judge Gabriel A. Fuentes **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **INJUNCTIVE RELIEF DEMANDED**

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Kylie S., Anthony P., Anna S. and Gena W., on behalf of themselves and as parents and guardians of their minor children, K.S., J.P., K.P., D.C., M.C., J.C., Z.W. and C.W., and on behalf of all other similarly situated individuals (collectively, "Plaintiffs"), by and through their attorneys, bring this Amended Class Action Complaint against Defendant Pearson plc; Defendant NCS Pearson, Inc. ("NCS"); and Defendant Pearson Education, Inc., doing business as Pearson Clinical Assessment ("Pearson Education") (all Defendants, collectively, "Pearson" or "Defendants"), and make the following allegations based upon knowledge as to themselves and their own acts, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. In November 2018, Pearson failed to exercise reasonable care in securing and safeguarding the sensitive data stored in its AIMSweb 1.0 platform ("AIMSweb") of over 900,000 children enrolled in, or who otherwise provided information to, approximately 13,000 schools and school districts in at least sixteen states across the United States resulting in the theft of that data (the "Data Breach). Among the data stolen was first and last names, dates of birth, email addresses and unique student identification numbers (collectively, "PII") of children who presently are known to be as young as four years of age. Defendants failed to have available systems in place to detect the breach on their own. Only after the Federal Bureau of Investigation informed Defendants of the Data Breach in March 2019 did Defendants begin to take action to secure the student data. Even then, Defendants wholly concealed their knowledge of the Data Breach from victim children and their parents and guardians until July 2019 – a time when Defendants knew many children were not in school and parents and guardians of students would not be focused on school issues. In disclosing the Data Breach, Defendants: (a) did not individually notify victim children or their parents and guardians of the breach; (b) failed to notify all impacted schools and school districts; and (c) concealed the true extent of the breach and Defendants' responsibility for the breach in order to minimize the impact on their reputations.

2. The Data Breach resulted from Defendants' failure to secure and protect the PII students were compelled to provide to Defendants. These students now have to live the rest of their lives knowing that criminals have the ability to compile, build and amass their profiles for decades – exposing them to a never-ending threat of identity theft, extortion, bullying and harassment.

3. Defendants disregarded the rights of Plaintiffs and Class and Sub-Class members (collectively, "Class Members") (the Class and Sub-Classes are defined below) by intentionally, willfully, recklessly or negligently: (a) failing to take adequate and reasonable measures to ensure the security of AIMSweb; (b) concealing or otherwise omitting the material fact that they did not have systems in place to safeguard student PII; (c) failing to take available steps to detect and prevent the Data Breach; (d) failing to monitor AIMSweb and to timely detect the Data Breach; and (e) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

4. As a result of Defendants' misconduct, the Data Breach compromised the PII of Plaintiffs and Class Members and made it available to criminals for misuse. The injuries suffered by Plaintiffs and Class Members as a direct result of the Data Breach include:

a. theft of personal information;

b. costs associated with the detection and prevention of identity theft;

c. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as time taken from the enjoyment of one's life, and the inconvenience, nuisance, cost and annoyance of dealing with all issues resulting from the Data Breach;

d. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web;

e. damages to, and diminution in value of, the PII that Defendants were supposed to keep secure; and

f. the loss of Plaintiffs' and Class Members' privacy.

5. Defendants directly and proximately caused the injuries suffered by Plaintiffs and Class Members by failing to implement or maintain adequate data security measures for PII.

6. Defendants have acknowledged the injuries, certainly impending injuries and damages caused by their actions by, among other things, offering temporary credit monitoring services to impacted students. The offered credit monitoring services are grossly inadequate because: (a) they fail to fully compensate Plaintiffs and Class Members for the injuries and damages they have suffered and will suffer far into the future; and (b) require Plaintiffs and Class Members to, among other things, reveal PII and waive certain legal rights in order to utilize them.

7. Plaintiffs retain a significant interest in ensuring that the breached PII, which remains in Defendants' possession, is protected from further breaches, and they seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated persons whose PII was stolen.

8. Plaintiffs, on behalf of themselves and on behalf of all other similarly situated persons, seek to recover damages, equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

PARTIES

9. Plaintiff Kylie S., individually and as parent and legal guardian for her minor child K.S., is an Illinois resident. K.S. attended a school within Downers Grove Grade School District 58 in Illinois that utilized AIMSweb. K.S.'s PII was compromised and stolen as a result of the Data Breach.

10. Plaintiff Anthony P., individually and as parent and legal guardian for his minor children J.P. and K.P., is an Illinois resident. J.P.and K.P. attend and attended a school within Downers Grove Grade School District 58 in Illinois that utilized AIMSweb. The PII of J.P. and K.P. was compromised and stolen as a result of the Data Breach.

11. Plaintiff Anna S., individually and as parent and legal guardian for her minor children D.C., M.C. and J.C., is a Colorado resident. D.C. and M.C. attend and attended schools within Boulder Valley School District in Colorado that utilized AIMSweb. In connection with a Colorado preschool program, J.C.'s PII was uploaded to AIMSweb by the Boulder Valley School District in Colorado. The PII of D.C., M.C. and J.C. was compromised and stolen as a result of the Data Breach.

12. Plaintiff Gena W., individually and as parent and legal guardian for her minor children C.W. and Z.W., is a Colorado resident. C.W. and Z.W. attend and attended schools within Boulder Valley School District in Colorado that utilized AIMSweb. The PII of C.W. and Z.W. was compromised and stolen as a result of the Data Breach.

13. Defendant Pearson plc is a for-profit, British corporation that, according to its 2018 Annual Report, operates in "70 markets worldwide" with North America being "its largest market including all 50 US states . . . ." Pearson plc has offices in San Antonio, Texas and Bloomington, Minnesota, among other places. Pearson plc holds itself out as the "world's learning company" and provides content, assessment and digital services to schools and seeks to grow its market share through digital transformation. At relevant times, Pearson plc had responsibility for AIMSweb and the way in which Pearson plc and all companies owned by Pearson plc – including Defendants Pearson Education and NCS – were to protect PII, which Pearson plc made known to its customers and potential customers, including customers and

potential customers in Illinois and Colorado. As recently as 2017, *Publisher's Weekly* listed Pearson as the largest publisher in the world. As of December 2018, Pearson plc reported total assets of approximately $9.683 billion.

14. Defendant Pearson Education, Inc., doing business as Pearson Clinical Assessment, is a Delaware corporation with a principal place of business in San Antonio, Texas that, among other things, provides student assessment testing that purportedly produces reliable information for guiding education decisions. Pearson Education, Inc. is a wholly-owned subsidiary of Pearson plc. The website "www.pearsonassessments.com" – which contains information about Pearson Clinical Assessment – is governed by Pearson Education's "Website Terms of Use." At relevant times, Pearson Education, Inc. operated in the United States and did business in Illinois and Colorado, among other places, including providing and overseeing AIMSweb services and having responsibility for AIMSweb.

15. Defendant NCS Pearson, Inc. is a Minnesota corporation, with its principal place of business in Bloomington, Minnesota, that markets application software for education, testing, assessment and complex data management. NCS Pearson, Inc. is a wholly-owned subsidiary of Pearson plc. At relevant times, NCS Pearson, Inc. operated in the United States and did business in Illinois and Colorado, among other places, including providing and overseeing AIMSweb services and having responsibility for AIMSweb.

JURISDICTION AND VENUE

16. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Classes. Based on published news reports, there are more

than 900,000 Class Members. Further, Defendants have already offered to provide Plaintiffs and Class Members with compensation in excess of $5,000,000, which offer is grossly inadequate and does not compensate Plaintiff and Class Members for, nor place a ceiling on, the full extent of injuries and damages sustained by Plaintiffs and Class Members as a result of the Data Breach. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

17. This Court has personal jurisdiction over Defendants because they are authorized to do business in this District and regularly conduct business in this District, have sufficient minimum contacts with this state and/or sufficiently avail themselves of the markets of this state through their promotion, sales, licensing and marketing within this state. Defendants purposely availed themselves of the laws of Illinois, and engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable and intended effect of causing injury to persons throughout the United States, including persons Defendants knew or had reason to know are located in Illinois (including in this District).

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (2) because the unlawful conduct alleged in this Class Action Complaint occurred in, was directed to and/or emanated in part from this District.

FACTUAL ALLEGATIONS

I. Data Breaches and the Market for PII.

19. Data breaches in the United States have become commonplace – almost 2,900 between 2017 and 2018.[1]

20. Criminals responsible for data breaches seek to monetize the stolen data.[2]

[1] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (accessed on August 22, 2019).

21. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data.[3]

22. According to Javelin Strategy & Research, in 2017 over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

23. The problem is compounded when companies entrusted with people's data fail to implement industry best practices because cyberattacks and other data exploitations can go undetected for long periods of time.

24. A person's identity is akin to a puzzle – the more accurate pieces a thief obtains about someone, the more the thief can take on the identity of the person and use software to figure out the person's passwords.[4] Armed with just a name and a date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more PII about a person, such as the person's login credentials and Social Security number merely by contacting the IT help desk of a company and pretending to be the person at issue.[5]

25. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information. The more information a data thief has about an individual, the better chance he/she has of obtaining additional confidential information.

26. PII is a valuable commodity for which a black market exists on the dark web, among other places. In this black market, criminals seek to sell the spoils of their cyberattacks to identity thieves who desire the data to extort and harass victims, take over victims' identities in

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *How Social Engineering Works and How to Protect Yourself*, available at https://usa.kaspersky.com/resource-center/definitions/social-engineering (accessed on September 29, 2019).

order to open financial accounts and otherwise engage in illegal financial transactions under the victims' names.

27. PII has a defined value – which is why legitimate companies and criminals seek to obtain and sell it. As alleged in more detail below, there is a growing market for children's data.[6]

28. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year.[7]

29. The U.S. Government Accountability Office has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[8] In the same report, the Government Accountability Office noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[9]

II. The Unique Nature of Student Data Commands Extra Vigilance in Protecting It.

30. Education technology platforms are popular targets for cyberattacks given the young age and vulnerability of the victims and the sensitive nature of the data stored therein.

---

[6] *The Worrying Trend of Children's Data Being Sold on the Dark Web*, available at https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/ (accessed on August 22, 2019).

[7] U.S. Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (Sept. 2015), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed on August 25, 2019).

[8] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services*, available at https://www.gao.gov/assets/700/697985.pdf (accessed on August 25, 2019).

[9] *Id.*

31. Criminals increasingly seek out children's data because children are less likely to check their credit reports or implement credit freezes, giving criminals longer periods of time to utilize a child's stolen identity.[10]

32. The FBI has warned that "widespread collection of student data could have privacy and safety implications if compromised or exploited."[11] According to the FBI, malicious use of sensitive student data "could result in social engineering, bullying, tracking, identity theft, or other means for targeting children."[12]

33. Three United States Senators recently expressed growing concern over stories and warnings involving breaches involving student data.[13] According to the Senators, a particularly alarming aspect of student data breaches is the fact that "students have little control over how their data is being collected and used. Students and parents are often unaware of the amount and type of data being collected about them and who may have access to it."[14]

34. Due to the special risks associated with student data breaches and the increasing frequency with which they are occurring, it is imperative for education technology companies like Pearson to routinely: (a) monitor for system breaches, cyberattacks and other exploitations; and (b) update their software, security procedures and firewalls.

---

[10] *See The Worrying Trend of Children's Data Being Sold on the Dark Web*, available at https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/ (accessed on August 22, 2019).

[11] *Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students*, FBI Alert No. I-091318-PSA (Sept. 13, 2018), available at https://www.ic3.gov/media/2018/180913.aspx (accessed on August 22, 2019).

[12] *Id.*

[13] A copy of one of the letters sent by the U.S. Senators to education technology companies is available at https://www.durbin.senate.gov/newsroom/press-releases/durbin-markey-blumenthal-request-information-on-student-data-collection-practices (accessed on August 22, 2019).

[14] *Id.*

III. The Data Breach.

35. AIMSweb was a digital education technology assessment platform licensed to schools and school districts by Defendants.

36. Students who were enrolled in a school or school district, or participated in a program through a school or school district, that utilized AIMSweb were subjected to the AIMSweb assessments as part of the school or school district's regular curriculum.

37. At relevant times, Plaintiffs and Class Members took reasonable steps to safeguard their PII.

38. Nevertheless, merely by attending school or enrolling in programs via a school or school district that utilized AIMSweb, Plaintiffs and Class Members were compelled to provide, and have provided, to Defendants valuable and sensitive PII, including, but not limited to, their first and last names, dates of birth, email addresses, unique student identification numbers, home addresses and telephone numbers.

39. Plaintiffs and Class Members relied on Defendants to keep their PII confidential and securely maintained, to solely use the information for educational purposes and to make only authorized disclosures of the information.

40. Notwithstanding the regularity with which data breaches were occurring in the United States and the FBI's concern with respect to student data, Defendants did not take the necessary steps to ensure that AIMSweb was secure and safe from cyberattack.

41. In March 2019, the FBI notified Defendants of a November 2018 cyberattack on AIMSweb that impacted approximately 13,000 accounts of schools and school districts containing the data of hundreds of thousands of students across the United States.

42. At no time between November 2018 and March 2019 did Defendants detect the cyberattack or Data Breach on their own or take any steps to fix the vulnerability that allowed for the breach.

43. Even after learning of the Data Breach in March 2019, Defendants concealed that fact from impacted schools, school districts, and victim students and their parents and guardians. Defendants did not begin disclosing the Data Breach to impacted schools and school districts until late July 2019 and, on information and belief, based on publicly available statements and documents, did not notify numerous schools and school district for many months after that. On information and belief, Defendants still have not notified all impacted schools and school districts.

44. In an effort to conceal the fact that Defendants were the parties responsible for the Data Breach, Defendants indicated in the disclosure notice alleged in paragraph 43, above, that the responsible party was "Pearson Clinical Assessment," an entity with no formal corporate existence and that is not listed in Pearson plc's Annual Report. The disclosure notice did, however, contain the Pearson plc logo and set forth a corporate address in San Antonio, Texas.[15]

45. Defendants also concealed the Data Breach from the public-at-large – delaying public notification until July 31, 2019. On or around that date, Defendants posted a notice on Defendant Pearson plc's website regarding the Data Breach. At no time have Defendants made any effort to individually notify Plaintiffs and Class Members of the Data Breach.

46. When Defendants finally gave notice of the Data Breach, they concealed and omitted material information about, and continue to conceal and omit material information about, the true extent and gravity of the Data Breach. As a result, the full extent and gravity of the Data Breach is still unknown to Plaintiffs and Class Members.

[15] Data Breach notification provided to impacted schools and school districts.

47. As an example of Defendants' concealment and omissions, the disclosure notice described in paragraphs 43 and 44, above, represented that the Data Breach was "isolated to first name, last name, and in some instances may include date of birth and/or email address,"[16] whereas in fact: (a) the Data Breach exposed other sensitive student data including – at a minimum – students' unique student identification numbers; and (b) the extent of the disclosure of dates of birth and email addresses was far greater than represented in the notice. Defendants also omitted the full extent of PII they collected and stored on AIMSweb.

48. Moreover, while the disclosure notice described in paragraphs 43 and 44, above, represented that "we do not have any evidence that this information has been misused" and that "we wanted to bring this to your attention as a precaution,"[17] Defendants concealed and omitted the true dangers to which Plaintiff and Class Members were exposed as a result of the Data Breach, which dangers Defendants knew. Moreover, Defendants concealed and omitted who was included in the term "we."

49. While Defendants downplayed the extent and gravity of the Data Breach, at the same time, they tacitly acknowledged the actual and certainly imminent injuries that victims of the Data Breach suffered and would suffer by initially offering to compensate victims in the form of one year of complimentary credit monitoring services.

50. The one year of offered credit monitoring services is grossly inadequate and fails to fully compensate Plaintiffs and Class Members for the injuries and damages they have suffered and will suffer far into the future, a fact Defendants have tacitly acknowledged.

[16] *Id.*
[17] *Id.*

IV. Defendants' Duty to Safeguard Student Data.

51. By obtaining, collecting, using and deriving a benefit from Plaintiffs and the Class Members' PII, Defendants assumed legal and equitable duties to those individuals, including the duty to protect Plaintiffs' and Class Members' PII from disclosure.

52. Beyond Defendants' legal obligations to protect the confidentiality of students' PII, at relevant times, Defendants affirmatively represented that they would safeguard their privacy. For example, Defendant Pearson plc made the following representations, among others:

> The data we collect could just be a name and an email address, but depending on your level of engagement with Pearson, it could be much more than that.
>
> * * *
>
> When you share your personal information with any company, you have a right to expect that information to be treated with total confidentiality.
>
> Your privacy is extremely important to us. We're committed to protecting any personal information you've given us, and we comply with all relevant data protection laws.
>
> This means that:
>
> - we take full responsibility for the information we hold about you
> - we will protect your privacy at all times
>
> * * *
>
> At Pearson, we know that you care how your personal information is used and we appreciate that you trust us to do that carefully and sensibly.
>
> * * *
>
> This Privacy Notice is provided on behalf of Pearson plc and its group companies.[18]

[18] "Pearson Privacy Statement," available at https://www.pearson.com/corporate/privacy-notice.html (accessed on October 4, 2019).

53. Defendant Pearson Education made the following representations, among others:

> We consider the following to be examples of personally identifying information: your first and last name, email address, home address, phone number, date of birth, social security number, credit card and banking information and other similar information.
>
> * * *
>
> **Special Notice to Parents, Teachers and Children**
>
> **Parents and Teachers:** When using this Service, we encourage parents, guardians and teachers to spend time with their children, especially if the child is 12 or under . . . WE ASK PARENTS TO HELP US PROTECT THEIR CHILREN'S PRIVACY BY INSTRUCTING THEM NEVER TO PROVIDE PERSONALLY IDENTIFIABLE INFORMATION ON THIS SERVICE WITHOUT FIRST GETTING PARENTAL/GUARDIAN OR TEACHER PERMISSION.
>
> **Children:** Please do not give your full name, email address, home address, telephone number, or any other personally identifiable information that would enable someone to contact you either online or offline, without first asking your parent/guardian or teacher for permission.[19]

54. At relevant times, Defendants knew: (a) the importance of safeguarding the student PII with which they were entrusted and which they knew was highly sensitive; and (b) the foreseeable consequences – and ensuing significant injuries – in the event of an AIMSweb data breach.

55. At relevant times, Defendants were aware or reasonably should have been aware that the PII collected, maintained and stored within AIMSweb was highly sensitive, susceptible to attack and, if improperly obtained, could be used by third parties for wrongful purposes such as identity theft and fraud.

[19] "Privacy Statement," available at https://www.pearson.com/us/privacy-statement.html (accessed on September 25, 2019).

56. At relevant times, Defendants knew, or reasonably should have known, of the significant volume of student data they received on a regular basis and the corresponding number of students who would be harmed by an AIMSweb breach.

57. At relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII, and of the foreseeable consequences that would occur in the event of an AIMSweb breach, including the significant cost that victims of such a breach would incur.

58. Notwithstanding Defendants' knowledge of the highly sensitive nature of the student PII they collected and the fact that they warned parents, teachers and children not to share that information, and notwithstanding all of the publicly-available information and knowledge regarding cyberattacks on education technology vendors and the corresponding dangers to students, Defendants were negligent or reckless in their approach to safeguarding the data stored within AIMSweb and the privacy of the students' data stored therein.

V. Defendants Failed to Comply with Federal Requirements

59. The Federal Trade Commission ("FTC") has instructed that the need for data security should be factored into all business decision-making.[20] To that the end, the FTC recommends that companies verify that third-party service providers have reasonable security measures in place; timely dispose of PII that is no longer needed; require the use of complex passwords on networks and monitor for suspicious activity thereon; and implement security methods that have been industry-tested.[21]

[20]Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (accessed on August 28, 2019).
[21] *Id.*

60. According to published FTC guidelines, businesses should: (a) protect customers' personal information – including encrypting information stored on computer networks and implementing policies to address security issues; (b) properly dispose of customer information when it is no longer needed; and (c) understand vulnerabilities on their network.[22] According to the guidelines, businesses should also have systems in place to detect intrusions and expose breaches as soon as they occur.

61. Pursuant to Section 5 of the FTC Act (15 U.S.C. § 45), the FTC has brought numerous actions against businesses for their failure to protect customer data, alleging that the conduct constitutes an unfair act or practice. The dispositions of these actions further inform the obligations of businesses when it comes to data security.

62. At relevant times, Defendants knew of their obligation to protect customer PII – especially given the fact that they were handling the PII of children – as well as the consequences of their failure to do so.

63. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice in violation of the FTC Act.

VI. Plaintiffs' and Class Members' Injuries and Damages.

64. As a result of the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer severe consequences, as they are more likely to become victims of social engineering, bullying, tracking, identity theft, and other means of targeting.

65. Defendants' failure to timely detect, and their deliberate delay in notifying students of the Data Breach, increased the risks and consequences Plaintiffs and Class Members

[22] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (accessed on August 28, 2019).

will suffer as a result of the Data Breach because cybercriminals had a head start to use the stolen data for their benefit and to the detriment of Plaintiffs and Class Members.

66. In order to prevent or limit the possibility of misuse of their PII, Plaintiffs and Class Members will have to take the following steps, among others:

a. Place a fraud alert on their credit bureau reports;

b. Place a security freeze on their credit bureau reports;

c. Periodically monitor their credit bureau reports for any unusual activity; and/or

d. Obtain and attempt to obtain new student identification numbers and change email addresses and account passwords.

67. Because data thieves often delay using stolen information, Plaintiffs and Class Members will continue to be at risk of the above-alleged harms well into the future.

68. Defendants' wrongful actions and inaction have directly and proximately caused Plaintiffs and Class Members to face the immediate and continuing increased risk of economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of personal information;

b. costs associated with the detection and prevention of identity theft;

c. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as time taken from the enjoyment of one's life, and the inconvenience, nuisance, cost and annoyance of dealing with all issues resulting from the Data Breach;

d. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web;

e. damages to, and diminution in value of, the PII that Defendants were supposed to keep secure; and

f. the loss of Plaintiffs' and Class Members' privacy.

CLASS ACTION ALLEGATIONS

69. Plaintiffs bring this action on behalf of themselves and their minor children and a class action under Federal Rules of Civil Procedure 23, seeking damages and equitable relief on behalf of the following nationwide Class for which Plaintiffs seek certification:

> All persons residing in the United States whose PII was provided to AIMSweb and whose PII was accessed without authorization as a result of the Data Breach (the "Nationwide Class").

70. Additionally, Plaintiffs Kylie S. and Anthony P. bring this action on behalf of an Illinois subclass seeking damages and equitable relief on behalf of the following:

> All persons residing in the State of Illinois whose PII was provided to AIMSweb and whose PII was accessed without authorization as a result of the Data Breach (the "Illinois Subclass").

71. Additionally, Plaintiffs Anna S. and Gena W. bring this action on behalf of a Colorado subclass seeking damages and equitable relief on behalf of the following:

> All persons residing in the State of Colorado whose PII was provided to AIMSweb and whose PII was accessed without authorization as a result of the Data Breach (the "Colorado Subclass").

72. Excluded from the Classes are: (a) Pearson, plc; NCS Pearson, Inc.; and Pearson Education, Inc.; (b) any parent, affiliate or subsidiary of Pearson plc; NCS Pearson, Inc. or Pearson Education, Inc.; (c) any entity in which Pearson plc; NCS Pearson, Inc. or Pearson

Education, Inc. has a controlling interest; (d) any of Pearson plc; NCS Pearson, Inc. or Pearson Education, Inc.'s officers or directors; or (e) any successor or assign of Pearson plc; NCS Pearson, Inc. or Pearson Education, Inc. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

73. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

74. **Numerosity.** Consistent with Rule 23(a)(1), the Classes are so numerous that joinder of all members is impracticable. While Plaintiffs do not know the exact number of members of the Classes, Plaintiffs believe the Nationwide Class contains over 900,000 people. Class Members may be identified through objective means, including objective data available to Defendants regarding whose PII was accessed without authorization as a result of the Data Breach. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media and/or published notice. All members of the Nationwide Class and Illinois and Colorado Subclasses are readily ascertainable because Defendants have access to information regarding the identity of each AIMSweb user.

75. **Commonality and predominance.** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Classes. Common questions include, but are not limited to the following:

a. Whether Defendants engaged in wrongful conduct as alleged herein;

b. Whether Defendants owed a duty to Plaintiffs and Class Members to adequately protect their PII and to provide timely and accurate notice of

the Data Breach to Plaintiffs and Class Members and whether Defendants willfully, recklessly or negligently breached these duties;

c. Whether Defendants willfully, recklessly or negligently failed to maintain and execute reasonable procedures to prevent unauthorized access to their data security networks and to Plaintiffs' and Class Members' PII;

d. Whether Defendants' conduct – including their failure to act – resulted in or was the proximate cause of the Data Breach;

e. Whether Defendants failed to inform Plaintiffs and Class Members of the Data Breach in a timely and accurate manner;

f. Whether Defendants continue to breach their duties to Plaintiffs and Class Members;

g. Whether Defendants have sufficiently addressed or remedied Plaintiffs' and Class Members' injuries and have taken adequate preventive and precautionary measures to ensure that Plaintiffs and Class Members will not experience further harm;

h. Whether Defendants' security measures to protect their computer systems were reasonable in light of the FTC data security recommendations and best practices recommended by security experts;

i. Whether Defendants failed to protect Plaintiffs and Class Members by allowing unauthorized access to their PII;

j. Whether Defendants engaged in unfair or deceptive trade practices by failing to disclose that they failed to properly safeguard Plaintiffs' and Class Members' PII;

k. Whether Plaintiffs and Class Members suffered damages as a proximate result of Defendants' conduct or failure to act; and

l. Whether Plaintiffs and Class Members are entitled to damages, equitable relief and other relief.

76. **Typicality.** Plaintiffs' claims are typical of the claims of the Nationwide Class, Illinois Subclass (as to Kylie S. and Anthony P.) and Colorado Subclass (as to Anna S. and Gena W.) they seek to represent because Plaintiffs and all members of the proposed Nationwide Class and Illinois and Colorado Subclasses have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests to advance adverse to the interests of the other members of the Nationwide Class and Illinois and Colorado Subclasses.

77. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the Nationwide Class, Illinois Subclass (as to Kylie S. and Anthony P.) and Colorado Subclass (as to Anna S. and Gena W.) and have retained as their counsel attorneys experienced in class actions and complex litigation.

78. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer management difficulties and provides the benefit of single adjudication, economy of scale and comprehensive supervision by a single court.

79. In the alternative, the proposed classes may be certified because:

a. The prosecution of separate actions by each individual member of the Nationwide Class and Illinois and Colorado Subclasses would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendants;

b. The prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class Members or which would substantially impair their ability to protect their interests; and

c. Defendants acted or refused to act on grounds generally applicable to the proposed classes, thereby making final and injunctive relief appropriate with respect to members of the Nationwide Class and Illinois and Colorado Subclasses as a whole.

80. Pursuant to Rule 23(c)(4) particular issues are appropriate for certification – namely the issues described in paragraph 75, above, because resolution of such issues would advance the disposition of the matter and the parties' interests therein.

CLAIMS FOR RELIEF

COUNT ONE
NEGLIGENCE
(On behalf of all Classes)

81. Plaintiffs restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

82. Defendants obtained Plaintiffs' and Class Members' PII and had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure.

83. Defendants also had a duty to destroy Plaintiffs' and Class Members' PII within an appropriate amount of time after it was no longer required by Defendants, in order to mitigate the risk of the stale PII being compromised in a data breach.

84. Further, Defendants had a duty to adequately protect AIMSweb and the PII stored thereon.

85. Once in possession and custody of Plaintiffs' and Class Members' PII within AIMSweb, Defendants undertook and owed a duty of care to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII – which they knew was private and confidential and should be protected as such – and to use commercially-reasonable methods to do so.

86. Defendants owed a duty of care not to subject Plaintiffs' and Class Members' PII or Plaintiffs and Class Members, themselves, to an unreasonable risk of harm from a data breach because Plaintiffs and Class Members were foreseeable and probable victims of inadequate security practices.

87. Defendants owed a duty of care to Plaintiffs and Class Members to quickly detect a data breach and to timely act on data breach warnings.

88. Defendants owed a duty to Plaintiffs and Class Members to timely and accurately disclose the Data Breach and the nature thereof.

89. Defendants' duties arose: (a) from their relationship to Plaintiffs and Class Members; (b) from their representations to Plaintiffs and Class Members; (c) out of their possession and custody of Plaintiffs and Class Members' PII; and (d) from industry custom.

90. Through their actions and/or failures to act, Defendants unlawfully breached duties owed to Plaintiffs and Class Members by failing to implement standard industry protocols

and failing to exercise reasonable care to secure and keep private the PII entrusted to them, including allowing unauthorized access to PII and failing to provide adequate oversight over the PII with which Defendants were entrusted despite knowing the foreseeable risk and likelihood of a data breach which would allow unauthorized third parties unfettered access to, and use of, Plaintiffs' and Class Members' PII without consent.

91. Through their actions and/or failures to act, Defendants allowed unmonitored and unrestricted access to unsecured PII.

92. Through their actions and/or failures to act, Defendants failed to provide adequate supervision and oversight of the PII with which they were entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather Plaintiffs' and Class Members' PII without consent.

93. Based on the publicity surrounding data breaches, at relevant times, Defendants knew or should have known the risks inherent in obtaining, collecting and storing PII and the concomitant necessity for adequate security measures to protect that PII.

94. At relevant times Defendants knew or should have known that AIMSweb and related systems failed to adequately safeguard Plaintiffs' and Class Members' PII, thereby creating a foreseeable risk that unauthorized third parties could and would gain access to Plaintiffs' and Class Members' PII.

95. Due to Defendants' knowledge that a breach of AIMSweb and related systems would damage hundreds of thousands of students, including Plaintiffs and Class Members, Defendants had a duty to adequately protect AIMSweb and the PII contained thereon.

96. Defendants had a special relationship with Plaintiffs and Class Members. Plaintiffs and Class Members were compelled to entrust Defendants with their PII. At relevant

times, Plaintiffs and Class Members understood that AIMSweb would take adequate security precautions to safeguard that information. Only Defendants had the ability to protect AIMSweb and the PII stored on AIMSweb and related systems from attack.

97. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII. Defendants' misconduct included failing to: (a) secure their computer systems, despite knowing their vulnerabilities; (b) comply with industry standard security practices; (c) implement adequate system and event monitoring; and (d) implement the systems, policies and procedures necessary to prevent this type of data breach.

98. Defendants breached the above-alleged duties to Plaintiffs and Class Members by, among other things: (a) failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII; (b) creating a foreseeable risk of harm through the above-alleged misconduct; (c) failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class Members' PII before and after learning of the Data Breach; (d) failing to utilize measures and practices that would allow for the timely detection of a data breach or other unauthorized access to PII within AIMSweb; (e) failing to comply with industry data security standards during the period of the Data Breach; and (f) failing to timely and accurately disclose that Plaintiffs' and Class Members' PII had been improperly acquired or accessed.

99. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of Plaintiffs' and Class Members' PII, so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

100. Defendants breached their duty to notify Plaintiffs and Class Members of the unauthorized access to their PII by failing to directly notify Plaintiff and Class Members and waiting to notify schools, school districts and the public, generally, and then by failing to provide sufficient or accurate information regarding the Data Breach.

101. Through Defendants' acts and omissions described herein, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' PII while it was within Defendants' possession or control.

102. On information and belief, Defendants improperly and inadequately safeguarded Plaintiffs' and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the unauthorized access. Defendants' failure to take proper security measures to protect sensitive PII as described herein created conditions conducive to a foreseeable, intentional criminal act – namely the unauthorized access of Plaintiffs' and Class Members' PII.

103. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including but not limited to: (a) failing to adequately protect the PII; (b) failing to conduct regular security audits; (c) failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' PII; and (d) failing to provide Plaintiffs and Class Members with timely and sufficient notice that their sensitive PII had been compromised.

104. Neither Plaintiffs nor other Class Members contributed to the Data Breach and subsequent misuse of their PII as described herein.

105. Defendants' failure to exercise reasonable care in safeguarding PII by adopting appropriate security measures, including proper encryption storage techniques, was the direct

and proximate cause of Plaintiffs' and Class Members' PII being accessed and stolen through the Data Breach.

106. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

107. As a direct and proximate result of Defendants' breach of duties, Plaintiffs and Class Members suffered damages including, but not limited to: (a) damages from lost time and the effort required to mitigate the actual and potential impact of the Data Breach on their lives, including by closely reviewing and monitoring their credit reports, placing freezes on their credit reports and attempting to obtain new student identification numbers; and (b) damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect. Based, in part, on Defendants' concealment and omission of material information related to the extent and gravity of the Data Breach, the full and potential scope of the Data Breach is not yet fully known and can only be assessed after a thorough investigation of the facts and events surrounding the theft alleged above.

COUNT TWO
(NEGLIGENCE *PER SE*)
(On behalf of all Classes)

108. Plaintiffs restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including the unfair act or practice by businesses of failing to use reasonable

measures to protect PII. The FTC publications and dispositions alleged above further define Defendants' duty under the FTC Act.

110. As alleged herein, Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the volume of PII they obtained and stored and the fact that much of the data was collected from minor children. The consequences of a data breach – including the damages Plaintiffs and Class Members would suffer – were foreseeable to Defendants.

111. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

112. Plaintiffs and Class Members are within the class of persons the FTC Act is intended to protect.

113. The harm that occurred as a result of the Data Breach is within the FTC's jurisdiction. As alleged herein, the FTC has brought enforcement actions against businesses that, like Defendants here, have failed to employ reasonable data security measures and engaged in unfair and deceptive practices, resulting in the same harm suffered by Plaintiffs and Class Members.

114. As a direct and proximate result of Defendants' breach of duties, Plaintiffs and Class Members suffered damages including, but not limited to: (a) damages from lost time and the effort required to mitigate the actual and potential impact of the Data Breach on their lives, including by closely reviewing and monitoring their credit reports, placing freezes on their credit reports and obtaining or attempting to obtain new student identification numbers; and (b) damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

115. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and adequate measures to protect that PII. The nature of other forms of economic damage and injury may take years to detect. Based, in part, on Defendants' concealment and omission of material information related to the extent and gravity of the Data Breach, the full and potential scope of the Data Breach can only be assessed after a thorough investigation of the facts and events surrounding the theft alleged above.

COUNT THREE
(BREACH OF EXPRESS CONTRACT)
(On behalf of all Classes)

116. Plaintiffs restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

117. Plaintiffs and Class Members' participation in AIMSweb was permitted pursuant to a standard licensing agreement (the "Express Contract") entered into between NCS and the schools and/or school districts in which Plaintiffs and Class Members were enrolled or to which they had provided their PII.

118. As consideration for the use of AIMSweb, the various schools and school districts paid fees to NCS.

119. The parties to the Express Contract intended Plaintiffs and Class Members to directly benefit from the Express Contract, as is apparent from the Express Contract's terms and surrounding circumstances. According to the Express Contract, one of its express purposes was to provide a "frequent and continuous assessment system designed to monitor student

achievement and instruction" for the clear purpose of improving student academic outcomes and benefitting students.

120. Plaintiffs and Class Members are third-party beneficiaries of the Express Contract.

121. Pursuant to the Express Contract, NCS was to take reasonable actions to ensure that the PII of Plaintiffs and Class Members was only disclosed to those authorized parties.

122. On information and belief, each school and/or school district in which Plaintiffs and Class Members were enrolled or had the PII of Plaintiff and Class Members fully performed its obligations under the Express Contract.

123. NCS breached the Express Contract by failing to employ reasonable and adequate privacy practices and measures, resulting in the disclosure of the PII of Plaintiffs and Class Members for purposes not required or permitted under the Express Contract.

124. As a direct and proximate result of NCS' breaches of the Express Contract, Plaintiffs and Class Members sustained actual losses as alleged above.

125. Plaintiffs and Class Members suffered harm as a result of NCS' breach of the Express Contract because their PII was compromised, placing Plaintiffs and Class Members at a greater risk of social engineering, bullying, tracking, identity theft, or other means of being targeted; and because their PII was disclosed to unauthorized third parties without their consent. Additionally, the value of Plaintiffs' and Class Members' PII has been diminished in that it is now in the hands of unauthorized third parties who can post it on the dark web or otherwise utilize it for their own interests.

126. Additionally, as a result of NCS' breach, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in

Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and adequate measures to protect that PII. The nature of other forms of economic damage and injury may take years to detect. Based, in part, on Defendants' concealment and omission of material information related to the extent and gravity of the Data Breach, the full and potential scope of the Data Breach can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

127. NCS' breach of the Express Contract was a direct and legal cause of Plaintiffs' and Class Members' injuries and damages as alleged above.

COUNT FOUR
BREACH OF IMPLIED CONTRACT
(On behalf of all Classes)

128. Plaintiffs restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

129. Defendants invited Plaintiffs and Class Members to use AIMSweb to improve their educational advancement, in part, by providing their PII. Plaintiffs and Class Members were compelled to accept Defendants' offer and provide their PII to Defendants.

130. When Plaintiffs and Class Members provided their PII to Defendants in return for the purported benefits of AIMSweb, Plaintiffs and Class Members, on the one hand, and Defendants, on the other, entered into mutually agreed-upon implied contracts pursuant to which Defendants agreed to utilize Plaintiffs' and Class Members' PII solely for the agreed-upon purpose of advancing their education.

131. In agreeing to solely use Plaintiffs' and Class Members' PII for the agreed-upon purpose of advancing Plaintiffs' and Class Members' education, Defendants further agreed they would use reasonable measures to safeguard Plaintiffs' and Class Members' PII.

132. Plaintiffs and Class Members fully performed their obligations under the implied contracts alleged above.

133. Defendants breached the implied contracts alleged above by failing to employ reasonable and adequate privacy practices and measures, resulting in the disclosure of the PII of Plaintiffs and Class Members for purposes not required or permitted under the implied contracts.

134. Defendants further breached the implied contracts alleged above by failing to provide timely and accurate notice to Plaintiffs and Class Members that their PII was compromised as a result of the Data Breach.

135. Defendants further breached the implied contracts alleged above by failing to ensure that the PII of Plaintiffs and Class Members was only used for the agreed-upon purpose of advancing their education.

136. As a direct and proximate result of Defendants' breaches of the implied contracts alleged above, Plaintiffs and Class Members sustained actual losses as alleged above.

137. Plaintiffs and Class Members suffered harm as a result of Defendants' breach of the implied contracts alleged above because their PII was compromised, placing Plaintiffs and Class Members at a greater risk of social engineering, bullying, tracking, identity theft, or other means of being targeted; and because their PII was disclosed to unauthorized third parties without their consent. Additionally, the value of Plaintiffs' and Class Members' PII has been diminished in that it is now in the hands of unauthorized third parties who can post it on the dark web or otherwise utilize it for their own interests.

138. Additionally, as a result of Defendants' breach, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants

fail to implement appropriate and adequate measures to protect that PII. The nature of other forms of economic damage and injury may take years to detect. Based, in part, on Defendants' concealment and omission of material information related to the extent and gravity of the Data Breach, the full and potential scope of the Data Breach can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

139. Defendants' breach of the implied contracts alleged above was a direct and legal cause of Plaintiffs' and Class Members' injuries and damages as alleged above.

COUNT FIVE
UNJUST ENRICHMENT
(On behalf of all Classes)

140. Plaintiffs restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

141. Plaintiffs and Class Members conferred a monetary benefit on Defendants – namely, they provided and entrusted their PII to Defendants.

142. In exchange, Plaintiffs and Class Members should have been entitled to have Defendants protect their PII with adequate data security.

143. Defendants appreciated, accepted and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiffs and Class Members as described herein – namely, (a) Plaintiffs and Class Members conferred a benefit on Defendants, and Defendants accepted or retained that benefit; and (b) Defendants used Plaintiffs' and Class Members' PII for business purposes.

144. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

145. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged, as well as failed to destroy or otherwise purge the PII from AIMSweb and related systems after Defendants no longer had a legitimate business purpose to maintain that PII.

146. Plaintiffs and Class Members have no adequate remedy at law.

147. Under the circumstances, it would be unjust and unfair for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred on them.

148. Under the principles of equity and good conscience, Defendants should not be permitted to retain the PII belonging to Plaintiffs and Class Members because Defendants failed to implement the data management and security measures that industry standards mandate.

149. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from the use of Plaintiffs' and Class Members' PII.

COUNT SIX
INTRUSION UPON SECLUSION
(On behalf of all Classes)

150. Plaintiffs restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

151. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to protection of this information against disclosure to unauthorized third parties.

152. Defendants owed a duty to AIMSweb users, including Plaintiffs and Class Members, to keep their PII confidential.

153. Defendants failed to protect Plaintiffs' and Class Members' PII stored within AIMSweb and related systems and released it to unknown and unauthorized third parties.

154. By way of Defendants' failure to protect the PII in AIMSweb and related databases, Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members.

155. The unauthorized release to, custody of and examination by unauthorized third parties of the PII of Plaintiffs and Class Members – especially where the information includes dates of birth and student identification numbers and relates to children – is highly offensive to a reasonable person.

156. The intrusion was into a place or thing that was private and entitled to be private. While Plaintiffs and Class Members were compelled to disclose their PII to Defendants as part of their use of Defendants' services, at all times the PII was supposed to be kept confidential and protected from unauthorized disclosure. It was reasonable for Plaintiffs and Class Members to believe that such information would be kept private and confidential and would not be disclosed without their authorization.

157. The Data Breach at the hands of Defendants constitutes an unauthorized intrusion or prying into Plaintiffs and Class Members' seclusion, and the intrusion was of a kind that would be highly offensive to a reasonable person.

158. Defendants acted with a knowing state of mind when they permitted the Data Breach because they had actual knowledge that their information security practices were inadequate and insufficient.

159. As a direct and proximate result of the above acts and omissions of Defendants, the PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages, anguish and suffering.

160. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendants can be viewed, distributed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT SEVEN
ILLINOIS PERSONAL INFORMATION AND PROTECTION ACT
815 ILCS § 530/1, *et seq.*
(On behalf of the Illinois Subclass)

161. Plaintiffs Kylie S. and Anthony P. ("Plaintiffs" for purposes of this Count) restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

162. As corporations that handle, collect, disseminate and otherwise deal with nonpublic personal information, Defendants are Data Collectors as defined in 815 ILCS § 530/5.

163. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Defendants violated 815 ILCS § 530/10(a).

164. Pursuant to 815 ILCS § 530/20, a violation of 815 ILCS § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

165. As a direct and proximate result of Defendants' violations of 815 ILCS § 530/10(a), Plaintiffs and Illinois Subclass Members suffered damages, as described above.

166. Plaintiffs and Illinois Subclass Members seek relief under 815 ILCS § 505/10(a) for the harm they suffered because of Defendants' willful violations of 815 ILCS § 530/10(a),

including actual damages, restitution, punitive damages, injunctive relief and reasonable attorneys' fees and costs.

COUNT EIGHT
ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 ILCS § 505/1, *et seq.*
(On behalf the Illinois Subclass)

167. Plaintiffs Kylie S. and Anthony P. ("Plaintiffs" for purposes of this Count) restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

168. Each Defendant is a "person" as defined by 815 ILCS § 505/1(c).

169. Defendants' conduct as alleged herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS § 505/1(f).

170. Defendants' deceptive, unfair and unlawful trade acts or practices, in violation of 815 ILCS § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, with each failure being a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a), and the Illinois Personal Information and Protection Act, 815 ILCS § 530/10(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a), and the Illinois Personal Information and Protection Act, 815 ILCS § 530/10(a), which was a direct and proximate cause of the Data Breach;

f. Omitting, suppressing and concealing the material fact that they did not reasonably or adequately secure Plaintiffs and Illinois Subclass Members' PII; and

g. Omitting, suppressing and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a), and the Illinois Personal Information and Protection Act, 815 ILCS § 530/10(a), which was a direct and proximate cause of the Data Breach.

171. Defendants' representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendants' data security and ability to protect the confidentiality of persons' PII.

172. Defendants intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

173. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to competition.

174. Defendants acted intentionally, knowingly and maliciously to violate Illinois' Consumer Fraud and Deceptive Business Practices Act and recklessly disregarded Plaintiffs and Illinois Subclass Members' rights.

175. As a direct and proximate result of Defendants' unfair, unlawful and deceptive practices and acts, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages, including from fraud and identity theft; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

176. Plaintiffs and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief and reasonable attorneys' fees and costs.

COUNT NINE
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 ILCS § 510/1, *et seq.*
(On behalf the Illinois Subclass)

177. Plaintiffs Kylie S. and Anthony P. ("Plaintiffs" for purposes of this Count) restate and reallege paragraphs 1 through 80, above, as though fully set forth herein.

178. Each Defendant is a "person" as defined by 815 ILCS § 510/1(5).

179. Defendants engaged in deceptive trade practices in the conduct of their businesses in violation of 815 ILCS § 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in conduct that creates a likelihood of confusion or misunderstanding.

180. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, with each failure being a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS § 505/2, and the Illinois Personal Information and Protection Act, 815 ILCS § 530/10(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS § 505/2, and the Illinois Personal Information and Protection Act, 815 ILCS § 530/10(a), which was a direct and proximate cause of the Data Breach;

f. Omitting, suppressing and concealing the material fact that they did not reasonably or adequately secure Plaintiffs and Illinois Subclass Members' PII; and

g. Omitting, suppressing and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS § 505/2, and the Illinois Personal Information and Protection Act, 815 ILCS § 530/10(a), which was a direct and proximate cause of the Data Breach.

181. Defendants' representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendants' data security and ability to protect the confidentiality of persons' PII.

182. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to competition.

183. As a direct and proximate result of Defendants' unfair, unlawful and deceptive trade practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages, including from fraud and identity theft; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

184. Plaintiffs and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees.

COUNT TEN
COLORADO SECURITY BREACH NOTIFICATION ACT
Colo. Rev. Stat. § 6-1-716, *et seq.*
(On behalf the Colorado Subclass)

185. Plaintiffs Anna S. and Gena W. ("Plaintiffs" for purposes of this Count") restate and reallege the allegations of paragraphs 1 through 80, above, as though fully set forth herein.

186. As businesses that maintain, own or license personal information in the course of their business, each Defendant is a covered entity under Colorado Revised Statute § 6-1-716(1).

187. The Data Breach resulted in the unauthorized acquisition of unencrypted computerized data that compromised the security, confidentiality and integrity of the personal information – as that term is defined in Colorado Revised Statute § 6-1-716(1) – of Plaintiffs and Colorado Subclass Members maintained by Defendants, including, on information and belief, first and last names in combination with student identification numbers, and therefore, constituted a security breach under Colorado Revised Statute § 6-1-716(1).

188. Pursuant to Colorado Revised Statute § 6-1-716(2), Defendants were required to accurately notify Plaintiffs and Colorado Subclass Members if they became aware of a breach of their data security systems in the most expedient time possible and without unreasonable delay.

189. Because Defendants were aware of a breach of their data security systems, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Colorado Revised Statute § 6-1-716(2).

190. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Colorado Revised Statute § 6-1-716(2).

191. As a direct and proximate result of Defendants' violations of Colorado Revised Statute § 6-1-716(2), Plaintiffs and Colorado Subclass Members suffered damages, as described above.

192. Plaintiffs and Colorado Subclass Members seek relief under Colorado Revised Statute § 6-1-716(4), including actual damages and equitable relief.

COUNT ELEVEN
COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §§ 6-1-101, *et seq.*
(On behalf the Colorado Subclass)

193. Plaintiffs Anna S. and Gena W. ("Plaintiffs" for purposes of this Count") restate and reallege the allegations of paragraphs 1 through 80, above, as though fully set forth herein.

194. Pearson plc is a person as defined by Colorado Revised Statute § 6-1-102(6).

195. NCS Pearson, Inc. is a person as defined by Colorado Revised Statute § 6-1-102(6).

196. Pearson Education, Inc. is a person as defined by Colorado Revised Statute § 6-1-102(6).

197. Defendants engaged in "sales" as defined by Colorado Revised Statute § 6-1-102(10).

198. Plaintiffs and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by Defendants or successors in interest to actual consumers.

199. Defendants engaged in deceptive trade practices in the course of their business, in violation of Colorado Revised Statute § 6-1-105(1), including:

a. Knowingly or recklessly making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality or grade, though Defendants knew or should have known that they were of another;

c. Advertising services with intent not to sell them as advertised;

d. Failing to disclose material information concerning their services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction; and

e. Knowingly or recklessly engaging in an unfair, unconscionable, deceptive, deliberately misleading, false or fraudulent act or practice.

200. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Colorado Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and to remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Colorado Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Colorado Security Notification Act, Colo. Rev. Stat. § 6-1-716(2), and the Colorado Student Data Transparency and Security Act, Colo. Rev. Stat. §§ 22-16-108 and 110, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and Colorado Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Colorado Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Colorado Security Notification Act, Colo. Rev. Stat. § 6-1-716(2), and the Colorado Student Data Transparency and Security Act, Colo. Rev. Stat. §§ 22-16-108 and 110, which was a direct and proximate cause of the Data Breach;

f. Omitting, suppressing and concealing the material fact that they did not reasonably or adequately secure Plaintiffs and Colorado Subclass Members' PII; and

g. Omitting, suppressing and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Colorado Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Colorado Security Notification Act, Colo. Rev. Stat. § 6-1-716(2), and the Colorado Student Data Transparency and Security Act, Colo. Rev. Stat. §§ 22-16-108 and 110, which was a direct and proximate cause of the Data Breach.

201. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

202. Defendants intended to mislead Plaintiffs and Colorado Subclass Members and induce them to rely on their misrepresentations and omissions;

203. Had Defendants disclosed to Plaintiffs and Colorado Subclass Members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business, and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants held themselves out as being committed to protecting personal information given to them while keeping the inadequate state of their security controls secret from the public. Plaintiffs and Colorado Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

204. Defendants acted intentionally, knowingly, recklessly and maliciously to violate Colorado's Consumer Protection Act and recklessly disregarded Plaintiffs and Colorado Subclass Members' rights.

205. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiffs and Colorado Subclass Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

206. Defendants' deceptive trade practices significantly impact the public because children and students throughout the State of Colorado are actual and potential consumers of Defendants' services and the Data Breach affected, at a minimum, over 60,000 Coloradans and at least 900,000 Americans.

207. Plaintiffs and Colorado Subclass Members seek all monetary and non-monetary relief allowed by law, including: (a) the greater of actual damages, $500 or three times actual damages (for Defendants' bad faith conduct); (b) injunctive relief; and (c) reasonable attorneys' fees and costs.

COUNT TWELVE
COLORADO STUDENT DATA TRANSPARENCY AND SECURITY ACT
Colo. Rev. Stat. §§ 22-16-101, *et seq.*
(On behalf the Colorado Subclass)

208. Plaintiffs Anna S. and Gena W. ("Plaintiffs" for purposes of this Count") restate and reallege the allegations of paragraphs 1 through 80, above, as though fully set forth herein.

209. As set forth in the Colorado Student Data Transparency and Security Act, Colo. Revised Statute § 22-16-101, *et seq.* (the "Student Data Security Act"), with the increasing use of technology in education, it is imperative that information that identifies individual students and their families is vigilantly protected from misappropriation and misuse that could harm students or their families.

210. Under Colorado Revised Statute § 22-16-103(7), AIMSweb was a school service in that it was: (a) an internet website, online service, online application or mobile application that

was designed and marketed primarily for use in a preschool, elementary school or secondary school; (b) used at the direction of teachers or other employees of a local education provider as that term is defined under Colorado Revised Statute § 22-16-103(4); and (c) collected, maintained or used student personally identifiable information as that term is defined under Colorado Revised Statute § 22-16-103(13).

211. As entities that entered into formal, negotiated contracts with public education entities to provide school services, Defendants were school-service contract providers under Colorado Revised Statute § 22-16-103(8).

212. Under Colorado Revised Statute § 22-16-103(13), the PII that was compromised in the Data Breach constituted student personally identifiable information in that the compromised PII, alone or in combination, personally identified individual students and was collected, maintained, generated or inferred by Defendants who were school service contract providers.

213. In violation of Colorado Revised Statute § 22-16-108, upon discovering the Data Breach, Defendants failed to notify the schools and/or school districts in which Plaintiffs and Colorado Subclass Members were enrolled or to which Plaintiffs and Colorado Subclass Members had provided their PII as soon as such notification was possible.

214. In violation of Colorado Revised Statute § 22-16-110, Defendants failed to maintain a comprehensive information security program that was reasonably designed to protect the security, privacy, confidentiality and integrity of student personally identifiable information and failed to make use of appropriate administrative, technological and physical safeguards.

215. In violation of Colorado Revised Statute § 22-16-110, Defendants failed to destroy student personally identifiable information after it was no longer needed.

216. Plaintiffs and Colorado Subclass Members are within the class of persons intended to be benefitted by the Student Data Security Act.

217. In adopting the Student Data Security Act, the Colorado legislature intended to create a private right of action.

218. A civil remedy under the Student Data Security Act would be consistent with the purposes of the legislative scheme set forth in that Act.

219. As a direct and proximate result of Defendants' violations of the Student Data Security Act, Plaintiffs and Colorado Subclass Members suffered damages, as described above.

220. Plaintiffs and Colorado Subclass Members seek relief under the Student Data Security Act, including actual damages and equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Kylie S., Anthony P., Anna S. and Gena W., on behalf of themselves and as parents and guardians of their minor children, K.S., J.P., K.P., D.C., M.C., J.C., Z.W. and C.W., and on behalf of the Classes, respectfully seek from the Court the following relief:

a. Certification of the Classes as requested herein;

b. Appointment of Plaintiffs as Class representatives and their undersigned counsel as Class counsel;

c. Award Plaintiffs and members of the proposed Classes damages;

d. Award Plaintiffs and members of the proposed Classes equitable, injunctive and declaratory relief, including the enjoining of Defendants' insufficient data protection practices at issue herein and Defendants' continuation of their unlawful business practices as alleged herein;

e. An order declaring that Defendants' acts and practices with respect to the safekeeping of PII are negligent;

f. Award Plaintiffs and members of the proposed Classes pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiffs and members of the proposed Classes reasonable attorneys' fees and costs of suit; including expert witness fees; and

h. Award Plaintiffs and members of the proposed Classes any further relief the Court deems proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: October 10, 2019

Respectfully submitted,

/s/ Scott R. Drury
SCOTT R. DRURY

Michael Kanovitz
Scott R. Drury
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
mike@loevy.com
drury@loevy.com

CERTIFICATE OF SERVICE

Scott R. Drury, an attorney, certifies that on October 10, 2019, he caused a true and correct copy of Amended Class Action Complaint to be filed using the Court's CM/ECF system, which effected service on all counsel of record.

/s/ Scott R. Drury
One of the attorneys for Plaintiffs